#3

Our Ref. No.: 51876.P225

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Dong-Cook Park et al.

Application No.: 09/752,668

Filed: 12/28/2000

For: **AGAINST DENIAL-OF-SERVICE ATTACK ON AUTHENTICATION PROTOCOLS USING PUBLIC KEY ENCRYPTION**

REQUEST FOR PRIORITY

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

Dear Sir:

Applicant respectfully requests a convention priority for the above-captioned application, namely Korean Patent Application No. 2000-74284 filed December 7, 2000. A certified copy of this document is submitted herewith.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Dated: 4/20/01 By: _____

Eric S. Hyman Reg. No. 30,139

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D.C. 20231 on _____ 2001

Lynda Shapiro Date

<Priority Document Translation>

THE KOREAN INDUSTRIAL

PROPERTY OFFICE

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

Application Number : 2000-74284 (Patent)

Date of Application : December 07, 2000

Applicant(s) : Korea Telecom

February 02, 2001

COMMISSIONER

CB042/US

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 2000년 제 74284 호
Application Number

출 원 년 월 일 : 2000년 12월 07일
Date of Application

출 원 인 : 한국전기통신공사
Applicant(s)

2001 년 02 월 02 일

특 허 청
COMMISSIONER

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【참조번호】 0002

【제출일자】 2000.12.07

【발명의 명칭】 공개키 암호화를 이용하는 인증 프로토콜에서의 서비스 거부공격에 대한 방어 방법

【발명의 영문명칭】 Countermeasure Against Denial of Service Attack in Authentication Protocols Using Public-Key Encryption

【출원인】

【명칭】 한국전기통신공사

【출원인코드】 2-1998-005456-3

【대리인】

【성명】 특허법인 신성 정지원

【대리인코드】 9-2000-000292-3

【포괄위임등록번호】 2000-050018-1

【대리인】

【성명】 특허법인 신성 원석희

【대리인코드】 9-1998-000444-1

【포괄위임등록번호】 2000-050018-1

【대리인】

【성명】 특허법인 신성 박해천

【대리인코드】 9-1998-000223-4

【포괄위임등록번호】 2000-050018-1

【발명자】

【성명의 국문표기】 박동국

【성명의 영문표기】 PARK,Dong Gook

【주민등록번호】 630916-1675917

【우편번호】 137-792

【주소】 서울특별시 서초구 우면동 17번지 한국통신연구개발본부 가입자망연 구소

【국적】 KR

【발명자】

【성명의 국문표기】 김정준

【성명의 영문표기】 KIM,Jung Joon

【주민등록번호】 590125-1695810

【우편번호】 137-792

【주소】 서울특별시 서초구 우면동 17번지 한국통신연구개발본부 가입자망연 구소

【국적】 KR

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 특허법인 신성 정지원 (인) 대리인 특허법인 신성 원석희 (인) 대리인 특허법인 신성 박해천 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	5	면	5,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	0	항	0 원
【합계】	34,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

1. 청구범위에 기재된 발명이 속한 기술분야

본 발명은 공개키 암호화를 이용하는 인증 프로토콜에서의 서비스거부공격에 대한 방어 방법에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은, 별도의 공개키 관련 계산을 수행할 필요없이, 서버의 공개키로 이용자(사용자 시스템) 난수를 암호화 함으로써 서버를 인증하는 어떤 프로토콜에도 적용이 가능한, 공개키 암호화를 이용하는 인증 프로토콜에서의 서비스거부공격에 대한 방어 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하고자 함.

3. 발명의 해결방법의 요지

본 발명은, 이용자가 서버를 인증하기 위해 난수를 서버의 공개키로 암호화한 암호문을 서버로 송신하는 통신시스템에서의 서비스거부공격에 대한 방어 방법에 있어서, 이용자 시스템의 서비스요구에 대하여 임의의 난수(r_B)를 발생하여, 상기 난수를 이용자 시스템으로 보내는 제 1 단계; 상기 이용자 시스템으로 보낸 임의의 난수(r_B)와 이용자가 가지고 있는 난수(r_A)를 이용하여 생성된 암호문을 수신하는 제 2 단계; 상기 이용자 시스템으로부터 수신된 암호문으로부터 난수(r_B) 값을 추출하여, 상기 추출된 난수 값과 상기 이용자 시스템으로 보낸 난수 값을 서로 비교하여 확인하는 제 3 단계; 및 상기 제 3 단계의 확인 결과, 상기 추출된 난수 값과 상기 이용자 시스템으로 보낸 난수

값이 같으면 서비스를 제공하고, 다르면 상기 이용자의 서비스 요구를 거부하는 제 4 단계를 포함함.

4. 발명의 중요한 용도

본 발명은 통신 시스템 등에 이용됨.

【대표도】

도 1

【색인어】

공개키, 암호화, 인증 프로토콜, 서비스거부공격(Denial-of-Service Attack)

【명세서】

【발명의 명칭】

공개키 암호화를 이용하는 인증 프로토콜에서의 서비스거부공격에 대한 방어 방법
{Countermeasure Against Denial-of-Service Attack in Authentication Protocols Using Public-Key Encryption}

【도면의 간단한 설명】

도 1 은 본 발명에 따른 공개키 암호화를 이용하는 인증 프로토콜에서의 서비스거부공격에 대한 방어 과정에 대한 일실시예 설명도.

도 2 는 본 발명에 따른 난수 생성 과정에 대한 일실시예 설명도.

도 3 은 본 발명에 따른 공개키 암호화를 이용하는 인증 프로토콜에서의 서비스거부공격 방어 과정에 대한 일실시예 흐름도.

도 4 는 본 발명에 따른 특수한 공개키 암호화를 이용한 인증 프로토콜에서의 서비스거부공격 방어 과정에 대한 일실시예 흐름도.

* 도면의 주요 부분에 대한 부호의 설명

100 : 서버 110 : 이용자(시스템)

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<7> 본 발명은 공개키 암호화를 이용하는 인증 프로토콜에서의 서비스거부공격에 대한 방어 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것으로, 더욱 상세하게는 인터넷 환경에서 일어나는 서비스거부공격을 해결하기 위하여 공개키 암호화를 통하여 서버를 인증하는 모든 인증 프로토콜에 적용할 수 있는 공개키 암호화를 이용하는 인증 프로토콜에서의 서비스거부공격에 대한 방어 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

<8> 인터넷 서비스가 널리 보급됨에 따라 서비스거부공격(Denial-of-Service Attack)이 사회적인 문제로 대두되고 있다. 특히, 실제 생활에서 일어나는 많은 일들이 가상공간인 인터넷에서도 일어나고 있으며, 서비스거부공격도 그 중의 하나이다.

<9> 상기 서비스거부공격은 해커, 즉 공격자가 짧은 시간 안에 많은 양의 접속 요구를 특정 서버에 보낸 후, 해당 세션들의 후속 메시지를 서버에 일부러 보내지 않음으로써 서버에서 세션들이 열린 채로 대기하게 만든다. 따라서, 서버는 일반 이용자(시스템)를 위한 세션을 더 이상 할당할 수 없게 된다.

<10> 이러한 공격의 대표적인 예로 TCP/IP(Transmission Control Protocol / Internet Protocol) 망에서의 SYN쇄도공격(SYN flood attack)을 들 수 있다.

<11> 상기 SYN쇄도공격은 TCP/IP 접속설정 프로토콜의 약점을 이용하는데, 상기 TCP/IP

접속설정을 위한 일반적인 절차는 다음과 같다.

<12> 먼저, 이용자(시스템)는 SYN 메시지를 서버로 보내고, 서버는 그 응답으로 SYN-ACK 메시지를 이용자(시스템)에게 보내면서 해당 세션을 위하여 서버 안에 버퍼 공간을 할당하게 된다. 상기 서버로부터 SYN-ACK 메시지를 받은 이용자(시스템)는 ACK 메시지를 보냄으로써 접속설정을 마치게 된다. 상기와 같은 과정을 거친 다음, 이용자(시스템)와 서버는 실제 서비스 데이터를 교환할 수 있다.

<13> 그러나, 공격자는 이러한 정상적인 절차를 그대로 따르지 않는다. 즉, 셋째 메시지인 SYN-ACK 메시지를 서버로 보내지 않는다. 따라서, 서버 안의 해당 세션은 타임아웃이 될 때까지 열린 채로 남아 있게 된다. 또한, 공격자는 한꺼번에 많은 양의 SYN 메시지를 특정 서버로 보냄으로써, 그 서버가 일반 이용자(시스템)의 접속 요구를 처리할 수 없게 만드는 것이다.

<14> 인터넷 환경에서 인증 프로토콜은 서비스거부공격 자체와는 별개의 문제라고 할 수 있다. 다시 말해서, 인증 프로토콜 자체는 서비스거부공격을 방지하는 데 아무런 도움이 되지 않는다. 오히려 인증 프로토콜 수행에 필요한 계산 부하 때문에 인증 프로토콜이 서비스거부공격의 또다른 대상이 되는 문제점이 있다.

<15> 상기 서비스거부공격에 대한 다른 방어책으로서 인터넷 서버를 주의 깊게 설계 운용함으로써 서비스거부공격의 피해를 최대한 줄일 수 있다. 그러나, 인증 프로토콜 자체의 취약성 때문에 또다른 서비스거부공격을 받을 수 있는 문제점이 있다.

<16> 또한, 서비스거부공격에 대한 다른 방어책으로서 암호학적인 방어 대책 방법이 있다.

<17> 상기 암호학적인 방어 대책은 새로운 연구분야로서, 서비스거부공격에 대한 '형식 논리학적 접근', 보안 프로토콜을 서비스거부공격에 대하여 더 튼튼하게 만드는 '영상태(stateless)프로토콜 설계 방법', 그리고 이용자(시스템)에게 일정 수준의 계산부하를 지움으로써 서비스거부공격을 완화하는 '이용자(시스템) 수수께끼(client puzzles) 방법' 등이 있다.

<18> 그러나, 상기 '이용자(시스템) 수수께끼(client puzzle) 방법'은 인증 프로토콜 자체와는 별도의 시스템으로 구현이 되어야 하는 단점이 있으며, 더욱이 이용자(시스템)와 서버 양쪽에 방어 기능을 위한 별도의 계산 부하가 필요한 약점이 있다.

<19> 암호학적 시도-응답(challenge-response) 메커니즘을 써서 서버를 인증하기 위해서는, 이용자가 임의의 난수를 선택해서 이를 서버 측에 전달한다. 이 난수를 처리하는 방법에 따라서, 인증 방법은 두 가지로 나눌 수 있다.

<20> 첫 번째 방법은, 이용자(시스템)가 난수를 서버에게 평문으로 전달하는 것이다. 서버는 이 값에 자신의 비밀 서명키를 적용하여 전자서명 데이터를 생성한 다음, 이를 이용자(시스템)에게 돌려 준다. 이용자(시스템)는 서버의 공개서명 확인키(public signature verification key)를 이용하여 전자서명 데이터를 검사하여 이 데이터가 해당 서버가 생성해서 보낸 것인 지를 확인한다. 이때, 성공적인 확인은 서버의 성공적인 인증을 뜻한다.

<21> 두 번째 방법에서는 이용자(시스템)가 난수를 서버의 공개 비화키(public encryption key)로 암호화하여 암호문으로 전달한다. 상기 암호문은 오로지 해당 서버만이 자신의 비밀키를 이용해서 복호화 할 수 있다. 상기 서버는 자신의 비밀키로 복호화된 평문 난수를 다시 이용자(시스템)에게 보낸다. 상기 이용자(시스템)는 자신이 서버로

보냈던 난수와 서버가 보내온 난수가 동일한 값인지를 확인한다. 확인이 성공하면 이는 서버 인증이 성공했다는 것을 뜻한다.

<22> 상기 두 가지 방법은 나름대로의 장단점이 있다. 그러나, 서비스거부공격에 관한 한 후자, 즉 난수를 암호화하는 방법이 더 우월하다. 왜냐하면, 서버가 이용자(시스템)로부터 받는 난수는 단순히 의미없는 난수가 아닌, 이 난수를 가공한 값, 즉 암호문이기 때문이다. 따라서, 이 암호화라는 가공처리 과정에 '서비스거부공격에 대한 방어'와 같은 기능을 추가할 수가 있다. 본 발명은 상기와 같은 부가 기능에 관한 것이다.

【발명이 이루고자 하는 기술적 과제】

<23> 본 발명은, 상기한 바와 같은 문제점을 해결하기 위하여 제안된 것으로, 별도의 공개키 관련 계산을 수행할 필요가 없으며, 서버의 공개키로 이용자(시스템) 난수를 암호화 함으로써 서버를 인증하는 어떤 인증 프로토콜에도 적용이 가능한, 서비스거부공격에 대한 방어 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있다.

【발명의 구성 및 작용】

<24> 상기 목적을 달성하기 위한 본 발명의 방법은, 이용자가 서버를 인증하기 위해 난수를 서버의 공개키로 암호화한 암호문을 서버로 송신하는 통신시스템에서의 서비스거부공격에 대한 방어 방법에 있어서, 이용자 시스템의 서비스요구에 대하여 임의의 난수(

r_B)를 발생하여, 상기 난수를 이용자 시스템으로 보내는 제 1 단계; 상기 이용자 시스템으로 보낸 임의의 난수(r_B)와 이용자가 가지고 있는 난수(r_A)를 이용하여 생성된 암호문을 수신하는 제 2 단계; 상기 이용자 시스템으로부터 수신된 암호문으로부터 난수(r_B) 값을 추출하여, 상기 추출된 난수 값과 상기 이용자 시스템으로 보낸 난수 값을 서로 비교하여 확인하는 제 3 단계; 및 상기 제 3 단계의 확인 결과, 상기 추출된 난수 값과 상기 이용자 시스템으로 보낸 난수 값이 같으면 서비스를 제공하고, 다르면 상기 이용자의 서비스 요구를 거부하는 제 4 단계를 포함하는 것을 특징으로 한다.

<25> 또한, 본 발명의 다른 방법은, 이용자가 시도응답(challenge-response)용 시도(challenge) 값으로, r_A대신 g^{r_A}와 같은 유한 멱승 계산결과를 이용하고, 서버의 개인키와 공개키가 각각 $b$dhk g^b이며, 서버 공개키를 이용한 이용자의 시도 값의 암호문이 g^{br_A}와 같은 특수한 경우의 서버 인증 시스템에 적용되는 서비스거부공격에 대한 방어 방법에 있어서, 이용자 시스템에 임의의 난수(r_B)를 보내는 제 1 단계; 상기 이용자 시스템으로 보낸 임의의 난수를 이용하여 계산된 하기의 수학식[1]의 x 값과 수학식[2]의 y값을 수신하는 제 2 단계; 상기 이용자 시스템으로부터 수신된 x와 y 값을 수학식[3]의 y'과 비교하여 확인하는 제 3 단계; 및 상기 제 3 단계의 확인 결과, 상기 y와 y'이 같으면 서비스를 제공하고, 다르면 상기 이용자 시스템의 서비스 요구를 거부하는 제 4 단계를 포함하는 것을 특징으로 한다.

<26> 한편, 본 발명은, 대용량 프로세서를 구비한, 이용자가 서버를 인증하기 위해 난수를 서버의 공개키로 암호화한 암호문을 서버로 송신하기 위한 통신시스템에, 이용자 시스템의 서비스요구에 대하여 임의의 난수(

r_B)를 발생하여, 상기 난수를 이용자 시스템으로 보내는 제 1 기능; 상기 이용자 시스템으로 보낸 임의의 난수(r_B)와 이용자 시스템이 가지고 있는 난수(r_A)를 이용하여 생성된 암호문을 수신하는 제 2 기능; 상기 이용자 시스템으로부터 수신된 암호문으로부터 난수를 추출하여, 상기 추출된 난수와 상기 이용자에게 보낸 난수를 서로 비교하여 확인하는 제 3 기능; 및 상기 제 3 기능의 확인 결과, 상기 추출된 난수와 상기 이용자(시스템) 시스템으로 보낸 난수가 같으면 서비스를 제공하고, 다르면 상기 이용자(시스템) 의 서비스 요구를 거부하는 제 4 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로-읽을 수 있는 기록매체를 제공한다.

<27> 또한, 본 발명은, 대용량 프로세서를 구비한, 이용자가 시도응답(challenge-response)용 시도(challenge) 값으로, r_A대신 g^{r_A}와 같은 유한 멱승계산결과를 이용하고, 서버의 개인키와 공개키가 각각 $b$dhk g^b이며, 서버 공개키를 이용한 이용자의 시도 값의 암호문이 g^{br_A}와 같은 특수한 경우의 서버 인증 시스템에, 이용자 시스템에 임의의 난수(r_B)를 보내는 제 1 기능; 상기 이용자 시스템으로 보낸 임의의 난수를 이용하여 계산된 상기의 수학식[1]의 x 값과 수학식[2]의 y값을 수신하는 제 2 기능; 상기 이용자 시스템으로부터 수신된 x와 y 값을 상기 수학식[3]의 y'과 비교하여 확인하는 제 3 기능; 및 상기 제 3 기능의 확인 결과, 상기 y와 y'이 같으면 서비스를 제공하고, 다르면 상기 이용자 시스템의 서비스 요구를 거부하는 제 4 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

<28> 상술한 목적, 특징들 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일

실시예를 상세히 설명한다.

<29> 도 1 은 본 발명에 따른 공개키 암호화를 이용하는 인증 프로토콜에서의 서비스거부공격에 대한 방어 과정에 대한 일실시예 설명도이다.

<30> 본 발명의 기본 개념은 이용자(시스템)가 자신이 생성한 난수를 서버 공개키로 암호화 할 때 서버가 생성한 난수도 함께 암호화하도록 하자는 것이다. 상기와 같은 난수 처리는 일반적인 난수 사용 방법에 비춰 볼 때 특이하다고 할 수 있다. 즉, 난수의 발생 및 전달의 목적은 상대방을 인증하는 시도 값(challenge value)으로 쓰고자 함인데, 본 발명에서는 상대방 즉, 이용자(시스템)가 암호문을 프로토콜에 따라 제대로 생성하였는지 아닌지를 구분하기 위한 용도로 사용하자는 것이다. 이용자(시스템)가 자신이 생성한 난수만 암호화해서 보낼 경우는 서버가 복호화하여도 상기 결과인 난수는 서버에게 이용자(시스템)의 암호문 생성 과정에 대하여 아무런 정보를 줄 수가 없다. 왜냐하면, 상기 난수는 의미없는 데이터이기 때문이다. 그 반면, 서버의 난수가 이용자(시스템)가 보내온 암호문 안에 포함되게 되면, 복호화 결과에 서버의 난수가 포함되어 있게 되고, 상기 사실이 서버로 하여금 이용자(시스템)가 암호문 생성을 프로토콜에 따른 적법한 생성을 하였다고 확신할 수 있게 해준다.

<31> 도 1 에 도시된 바와 같이, 먼저 서버(100)는 난수 r_B(101)를 생성하여 이용자(시스템)(110)에게 보낸다.

<32> 상기 서버(100)로부터 난수 r_B(101)를 받은 이용자(시스템)(110)는 난수 r_A(111)를 생성하여 이 두 난수 r_B(101)와 r_B(111)를 서버(100)의 공개키 K_B로 암호화한 암호문(112)을 서버(100)로 보낸다.

<33> 상기 서버(100)는 이용자(시스템)(시스템)(110)로부터 수신한 암호문(112)을 복호화하여 난수 r_B(101)와 난수 r_A(111)를 추출한다.

<34> 상기 추출된 난수 r_B의 값은 서버(100)가 이용자(시스템)(110)에게 송신했던 난수 r_B(101)의 값과 비교한다. 이때, 상기 추출된 난수 r_B의 값은 서버(100)가 이용자(시스템)(110)에게 송신했던 난수 r_B(101)의 값은 일치해야 한다. 만약 일치하지 않는다면, 이것은 수신된 암호문(112)이 프로토콜에 부합하는 올바른 암호문이 아니라 공격자가 보낸 불용정보(garbage value)인 것이다.

<35> 상기 추출된 난수 r_B의 값은 서버(100)가 이용자(시스템)(110)에게 송신했던 난수 r_B(101)의 값과 일치하면 인증 프로토콜에 규정된 다음 단계를 수행하게 된다.

<36> 한편, 상기와 같은 방어 절차가 없다면, 서버가 수신한 암호문이 프로토콜에 부합하는 값인지, 아니면 단순히 불용정보인지를 확인할 수 있는 방법이 없으며, 공격자가 보낸 불용정보에 대해서도 서버는 프로토콜 절차에 따라 복호화를 위한 공개키 연산과 후속 프로토콜 메시지를 보낸 다음, 공격자로부터 응답을 기다리면서 해당 세션을 열어 놓게 된다. 물론, 공격자는 응답 메시지를 보내지 않으므로, 이 세션은 시간경과(time out)에 의해 종료될 때까지 서버 시스템의 자원을 낭비하게 된다.

<37> 상기 방법을 이용함으로써 별도의 공개키 관련 계산을 수행할 필요가 전혀 없으며, 서버의 공개키로 이용자 난수를 암호화함으로써 서버를 인증하는 어떤 프로토콜에도 적용이 가능하다.

<38> 도 2 는 본 발명에 따른 난수 생성 과정에 대한 일실시예 설명도이다.

<39> 난수 r_B의 생성 방법에 따라 서비스거부공격에 대한 서버의 면역성을 더욱 강화할

수도 있다.

<40> 서버(100)는 난수 r_B(101)를 이용자(시스템)(110)에게 송신한 뒤에 그 이용자(시스템)(110)를 위하여 고유한 세션을 할당하는 것이 보통이다. 여기서, 난수 r_B(101)의 값은 서버의 해당 세션에 고유한 값으로 할당되어 있다. 상기 난수 r_B(101)값은 저장되어 있다가, 이용자(시스템)(110)가 보내온 난수 r_B값과 비교된다.

<41> 그러나, 상기와 같은 난수관리 방식의 문제점은 TCP/IP환경에서의 SYN쇄도공격을 가능하게 하는 문제점과 본질적으로 같다고 할 수 있다. 따라서, 상기 문제를 해결하는 방법은 다음과 같다.

<42> 즉, 서버는 이용자(시스템)가 보내온 암호문이 프로토콜에 부합하는 올바른 암호문인지를 검증하기 전까지는 시스템 자원을 이용자(시스템)에게 할당하지 않는 것이다. 다시 말해서, 이용자(시스템)가 올바른 암호문을 보내기 전에는 서버가 특정 난수 r_B값을 해당 이용자(시스템)에게 할당하지 않아야 한다.

<43> 여기서, 특정 난수 r_B를 생성하는 방법은 다음과 같다.

<44> 도 2 에 도시된 바와 같이, 임의의 마스터키(K_{master}, 201)와 난수 r_B의 인덱스($index\_r_B$, 202)를 해쉬함수(H, 200)의 입력값으로 취하여 난수 r_B(203)를 생성한다.

<45> 여기서, 난수 r_B의 인덱스($index\_r_B$, 202)의 값은 최소 0부터 최대 M-1까지가 되며, 여기서 M은 난수 r_B의 인덱스($index\_r_B$, 202)를 위한 계수이다.

<46> 즉, 새로운 난수 r_B값을 생성할 때마다 서버는 마스터키(K_{master}, 201)와 난수 r_B

의 인덱스($index\_r_B$, 202)값을 입력치로 취하여 해쉬함수를 계산하게 된다. 그리고, 그 결과 값을 난수 r_B에 할당하게 된다.

<47> 도 3 은 본 발명에 따른 공개키 암호화를 이용하는 인증 프로토콜에서의 서비스거부공격 방어 과정에 대한 일실시예 흐름도이다.

<48> 먼저, 이용자(시스템)(320)로부터 서비스 요구(321)를 받은 서버(310)는 난수 r_B(330)를 다음과 같은 연산에 의하여 생성한다.

<49> $$r_B=H(K_{master}, index\_r_B)$$

<50> 다음으로, 상기 서버는 생성된 난수 r_B(330)와 난수 r_B의 인덱스($index\_r_B$)를 이용자(시스템)에게 송신하고(331), 상기 난수 r_B의 인덱스($index\_r_B$)의 값을 증가시킨다(350).

<51> 상기 난수 r_B와 난수 r_B의 인덱스($index\_r_B$)를 받은 이용자(시스템)(320)는 자신의 난수 r_A를 생성하여 이를 난수 r_B와 함께 암호화한다(340). 이때 이용하는 암호키는 서버의 공개키 K_B이다. 여기서, 난수 r_A와 난수 r_B를 서버의 공개키 K_B로 암호화한 암호문은 $\{r_A, r_B\}_{K_B}$와 같이 표기한다.

<52> 상기 이용자(시스템)(320)는 상기 암호문($\{r_A, r_B\}_{K_B}$)을 난수 r_B의 인덱스($index\_r_B$)와 함께 서버(310)로 송신한다(341).

<53> 상기 이용자(시스템)(320)로부터 암호문($\{r_A, r_B\}_{K_B}$)을 받은 서버(310)는 수신한 난수 r_B의 인덱스($index\_r_B$)의 값을 이용하여 검색 테이블(look up table)을 검색하여 해당 난수 r_B값을 찾거나, 또는 난수 생성식인 $r_B=H(K_{master}, index\_r_B)$ 의 관계식으로부터 난

수 r_B값을 다시 계산할 수 있다(360).

<54> 상기 서버(310)는 수신한 암호문($\{r_A, r_B\}K_s$)을 해독하여 난수 r_B값을 추출하고, 상기 추출된 값을 앞에서 검출 또는 재계산한 난수 r_B 값과 일치하는지 확인한다(370).

<55> 확인한 결과, 두 값이 일치하면 서버(310)는 이용자(시스템)(320)가 프로토콜에 부합하는 암호문($\{r_A, r_B\}K_s$)을 올바르게 생성하여 보낸 것으로 확신할 수 있다. 따라서, 서버는 인증 프로토콜에 규정된 다음 단계를 수행하면 된다(380).

<56> 확인한 결과, 두 값이 일치하지 않으면 서버는 이용자(시스템)가 프로토콜에 규정된 암호문($\{r_A, r_B\}K_s$)과는 전혀 무관한 불용정보, 즉 가짜 암호문을 보낸 것으로 판단할 수 있다. 물론, 이 이용자(시스템)는 서비스거부공격을 시도하고 있는 것이다. 따라서, 서버는 즉시 이 세션을 중단하고 빠져나간다(390).

<57> 도 4 는 본 발명에 따른 특수한 공개키 암호화를 이용한 인증 프로토콜에서의 서비스거부공격 방어 과정에 대한 일실시예 흐름도이다.

<58> 이산대수(discrete logarithm)에 기반을 둔 암호화 기법을 이용하는 프로토콜의 경우, 이용자(시스템) 생성 난수를(여기서는 r_A대신 g^{r_A}를 송신 값으로 이용) 암호화하기 위해 g^{br_A}와 같은 형태를 이용할 수도 있다. 여기서, g는 이용자(시스템)-서버간에 약속된 특정 유한 사이클릭 그룹(finite cyclic group)의 생성자(generator)이며 b와 g^b는 각각 서버의 개인키와 공개키이다. 이러한 특수한 형태의 암호화 방식에 대해서는 도 1에 기술된 절차를 적용하는 것이 용이하지 않다. 여기서, 문제는 추가적인 공개키 관련 멱승(exponentiation)계산이 없어야 한다는 것이다.

<59> 상기 문제는 다음과 같은 방법으로 해결한다.

<60> 서버(400)는 서비스를 요구한 이용자(시스템)(400)에게 난수 r_B(401)를 송신한다.

<61> 상기 난수 r_B(401)를 수신한 이용자(시스템)(410)는 $x=(g^b)^{r_A+r_B}$와 $y=h(g^{r_A})$(411)를 계산하여 이 값들을 서버(400)로 송신한다. 여기서, h는 서버(400)와 이용자(시스템)(410) 간에 미리 약속된 해쉬 함수다.

<62> 상기 x와 y(411)를 수신한 서버(400)는 $y'=h(x^{b^{-1}}g^{-r_B})$를 계산하여(420), y와 y'의 값이 서로 일치하는지 확인한다(430).

<63> 확인한 결과, 만약 두 값이 일치하면 서버는 이용자(시스템)가 프로토콜에 부합하는 올바른 공개키 연산의 결과를 보내온 것으로 판단할 수 있다. 따라서, 서버는 인증을 위한 프로토콜에 규정된 다음 단계를 수행하면 된다(440).

<64> 확인한 결과, 두 값이 서로 다르면 이용자(시스템)가 불용정보를 보내서 서비스거부공격을 시도하고 있는 것으로 판단하고 세션을 즉시 닫고 빠져나온다(450).

<65> 상기 과정에서, 이용자(시스템)(410) 측의 추가 공개키 연산은 없다. 다만, 서버(400)의 경우 g^{-r_B}와 같은 멱승 계산이 한개 더 늘어난다. 그러나, 이 계산은 서버가 온라인이 아닌 오프라인으로 처리할 수 있다. 따라서, 실제 운용시 난수 r_B의 생성이나 g^{-r_B}계산은 일괄작업(batch job)으로 처리할 수 있을 것이다. 참고로, $y'=h(x^{b^{-1}}g^{-r_B})$의 계산에 필요한 멱승계산인 $x^{b^{-1}}$는 별도 계산이 아니라, 어차피 거쳐야 할 계산이다. 왜냐하면, 이러한 방어 절차를 운용하지 않더라도 서버(400)는 g^{r_A}를 추출하기 위해 $(g^{br_A})^{b^{-1}}=g^{r_A}$와 같은 멱승계산이 한 번 필요하기 때문이다. 따라서, 방어 절차 수행에 필요한 중간 값인 $x^{b^{-1}}g^{-r_B}=g^{r_A}$는 멱승계산을 추가로 요구하지 않음을 알 수 있다.

<66> 지금까지 기술된 과정들은 이용자(시스템)가 공개키 암호화를 이용하여 서버를 인

증하는 어떤 프로토콜에도 적용될 수 있다.

<67> 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다.

<68> 이상에서 설명한 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하다는 것이 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 명백할 것이다.

【발명의 효과】

<69> 상기한 바와 같은 본 발명은, 서비스거부공격에 대한 면역성을 인증 프로토콜 자체에 부여하며, 별도의 공개키 관련 계산을 수행할 필요가 없으며, 서버의 공개키로 이용자(시스템) 난수를 암호화 함으로써 서버를 인증하는 어떤 프로토콜에도 적용이 가능하며 서비스거부공격에 대한 방어에 효과가 있다.

【특허청구범위】

【청구항 1】

이용자가 서버를 인증하기 위해 난수를 서버의 공개키로 암호화한 암호문을 서버로 송신하는 통신시스템에서의 서비스거부공격에 대한 방어 방법에 있어서,

이용자 시스템의 서비스요구에 대하여 임의의 난수(r_B)를 발생하여, 상기 난수를 이용자 시스템으로 보내는 제 1 단계;

상기 이용자 시스템으로 보낸 임의의 난수(r_B)와 이용자가 가지고 있는 난수(r_A)를 이용하여 생성된 암호문을 수신하는 제 2 단계;

상기 이용자 시스템으로부터 수신된 암호문으로부터 난수(r_B) 값을 추출하여, 상기 추출된 난수 값과 상기 이용자 시스템으로 보낸 난수 값을 서로 비교하여 확인하는 제 3 단계; 및

상기 제 3 단계의 확인 결과, 상기 추출된 난수 값과 상기 이용자 시스템으로 보낸 난수 값이 같으면 서비스를 제공하고, 다르면 상기 이용자의 서비스 요구를 거부하는 제 4 단계

를 포함하는 서비스거부공격에 대한 방어 방법.

【청구항 2】

제 1 항에 있어서,

상기 제 1 단계는,

임의의 난수 r_B 대신에 하기의 수학식에 의하여 구한 난수 r_B를 상기 이용자 시스템으로 송신하는 것을 특징으로 하는 서비스거부공격에 대한 방어 방법.

$$r_B = H(K_{master}, index\_r_B)$$

(여기서, H는 해쉬 함수, K_{master}는 비밀 마스터 키, $index_r_B$는 난수 r_B를 위한 색인 파라미터)

【청구항 3】

이용자가 시도응답(challenge-response)용 시도(challenge) 값으로, r_A대신 g^{r_A}와 같은 유한 멱승 계산결과를 이용하고, 서버의 개인키와 공개키가 각각 $b$dhk g^b이며, 서버 공개키를 이용한 이용자의 시도 값의 암호문이 g^{br_A}와 같은 특수한 경우의 서버 인증 시스템에 적용되는 서비스거부공격에 대한 방어 방법에 있어서,

이용자 시스템에 임의의 난수(r_B)를 보내는 제 1 단계;

상기 이용자 시스템으로 보낸 임의의 난수를 이용하여 계산된 하기의 수학식[1]의 x 값과 수학식[2]의 y값을 수신하는 제 2 단계;

상기 이용자 시스템으로부터 수신된 x와 y 값을 수학식[3]의 y'과 비교하여 확인하는 제 3 단계; 및

상기 제 3 단계의 확인 결과, 상기 y와 y'이 같으면 서비스를 제공하고, 다르면 상기 이용자 시스템의 서비스 요구를 거부하는 제 4 단계

를 포함하는 서비스거부공격에 대한 방어 방법.

【수학식 1】

$$x=(g^{b})^{r_A+r_B}$$

(여기서, b는 서버의 개인키, g^{b}는 서버의 공개키)

【수학식 2】

$$y=h(g^{r_A})$$

(여기서, h는 해쉬함수)

【수학식 3】

$$y'=h(x^{b^{-1}}g^{-r_B})$$

(여기서, h는 해쉬함수)

【청구항 4】

대용량 프로세서를 구비한, 이용자가 서버를 인증하기 위해 난수를 서버의 공개키로 암호화한 암호문을 서버로 송신하기 위한 통신시스템에,

이용자 시스템의 서비스요구에 대하여 임의의 난수(r_B)를 발생하여, 상기 난수를 이용자 시스템으로 보내는 제 1 기능;

상기 이용자 시스템으로 보낸 임의의 난수(r_B)와 이용자 시스템이 가지고 있는 난수(r_A)를 이용하여 생성된 암호문을 수신하는 제 2 기능;

상기 이용자 시스템으로부터 수신된 암호문으로부터 난수를 추출하여, 상기 추출된 난수와 상기 이용자에게 보낸 난수를 서로 비교하여 확인하는 제 3 기능; 및

상기 제 3 기능의 확인 결과, 상기 추출된 난수와 상기 이용자(시스템) 시스템으로 보낸 난수가 같으면 서비스를 제공하고, 다르면 상기 이용자(시스템)의 서비스 요구를 거부하는 제 4 기능

을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【청구항 5】

대용량 프로세서를 구비한, 이용자가 시도응답(challenge-response)용 시도(challenge) 값으로, r_A대신 g^{r_A}와 같은 유한 멱승 계산결과를 이용하고, 서버의 개인키와 공개키가 각각 $b$dhk g^b이며, 서버 공개키를 이용한 이용자의 시도 값의 암호문이 g^{br_A}와 같은 특수한 경우의 서버 인증 시스템에,

이용자 시스템에 임의의 난수(r_B)를 보내는 제 1 기능;

상기 이용자 시스템으로 보낸 임의의 난수를 이용하여 계산된 상기의 수학식[1]의 x 값과 수학식[2]의 y값을 수신하는 제 2 기능;

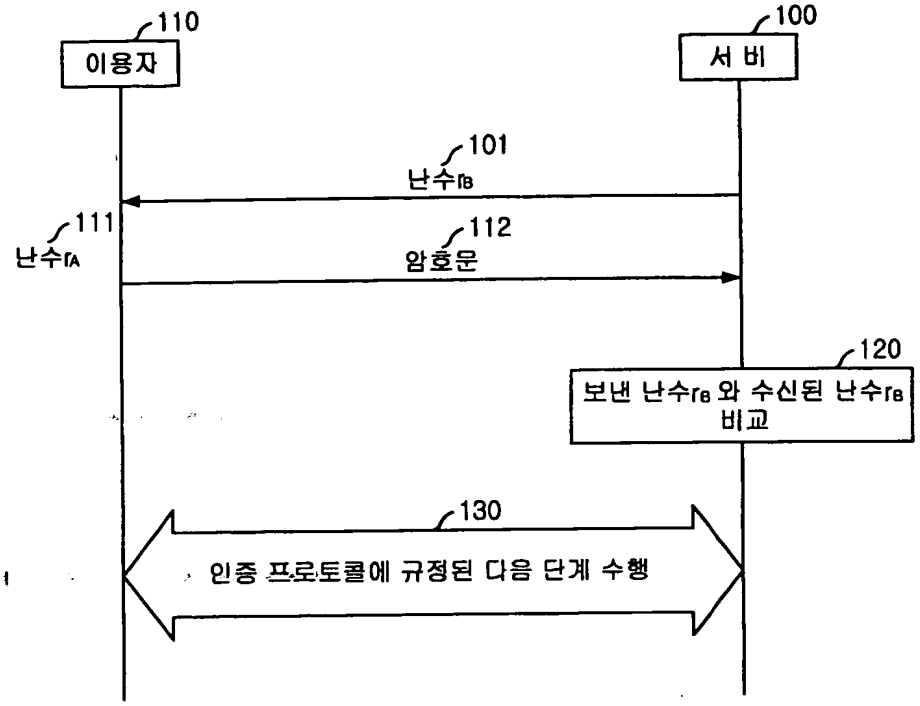
상기 이용자 시스템으로부터 수신된 x와 y 값을 상기 수학식[3]의 y'과 비교하여 확인하는 제 3 기능; 및

상기 제 3 기능의 확인 결과, 상기 y와 y'이 같으면 서비스를 제공하고, 다르면 상기 이용자 시스템의 서비스 요구를 거부하는 제 4 기능

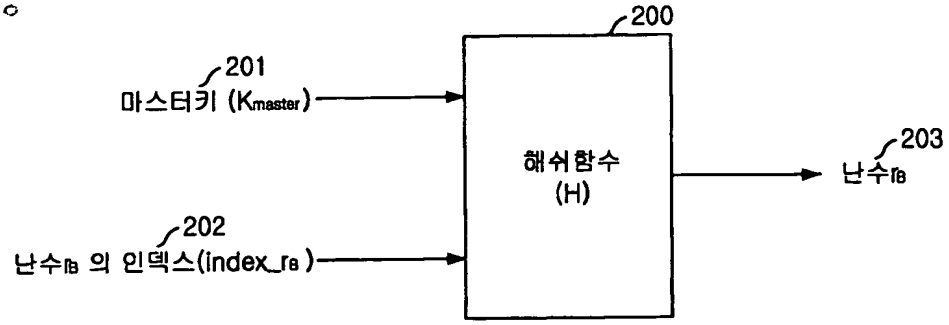
을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

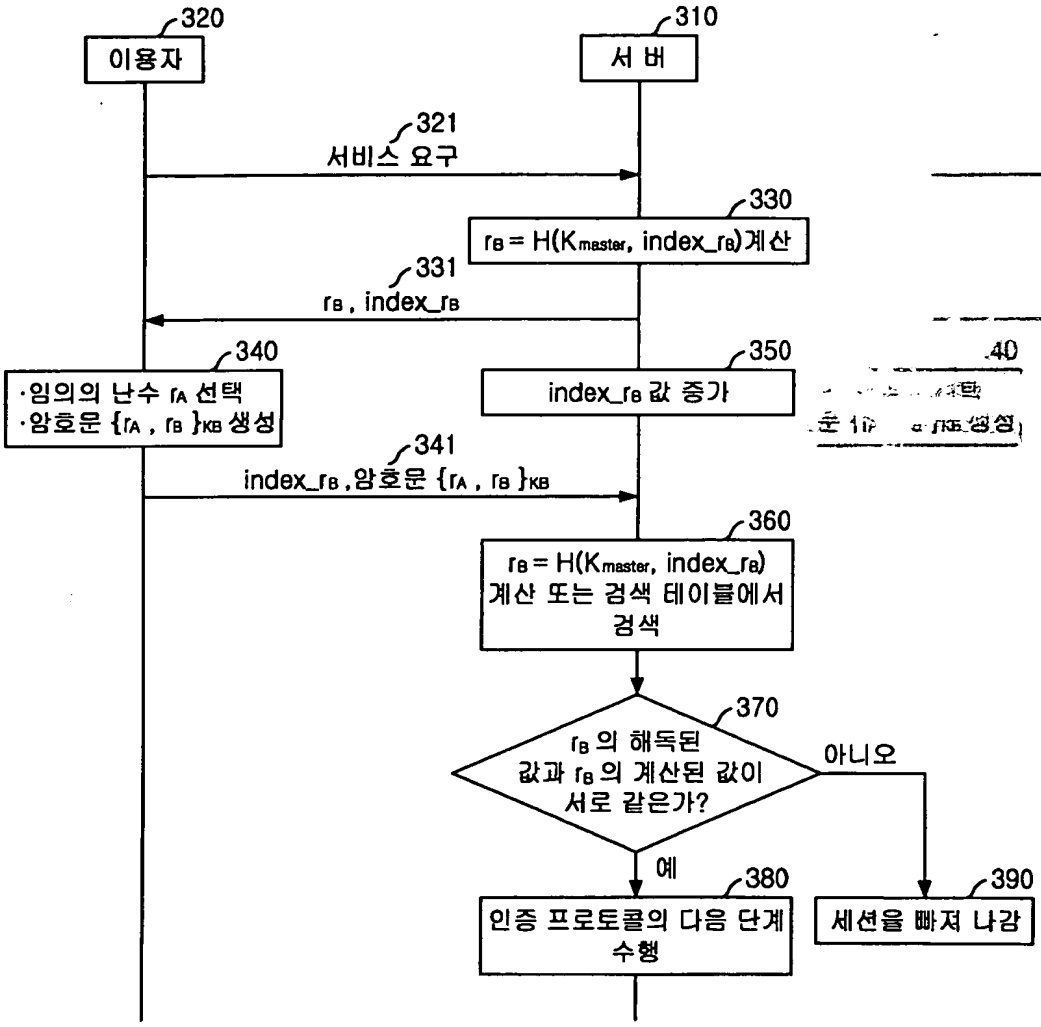
【도 1】


110
이용자
100
서 비
101
난수r_B
111
난수r_A
112
암호문
120
보낸 난수r_B와 수신된 난수r_B 비교
130
인증 프로토콜에 규정된 다음 단계 수행

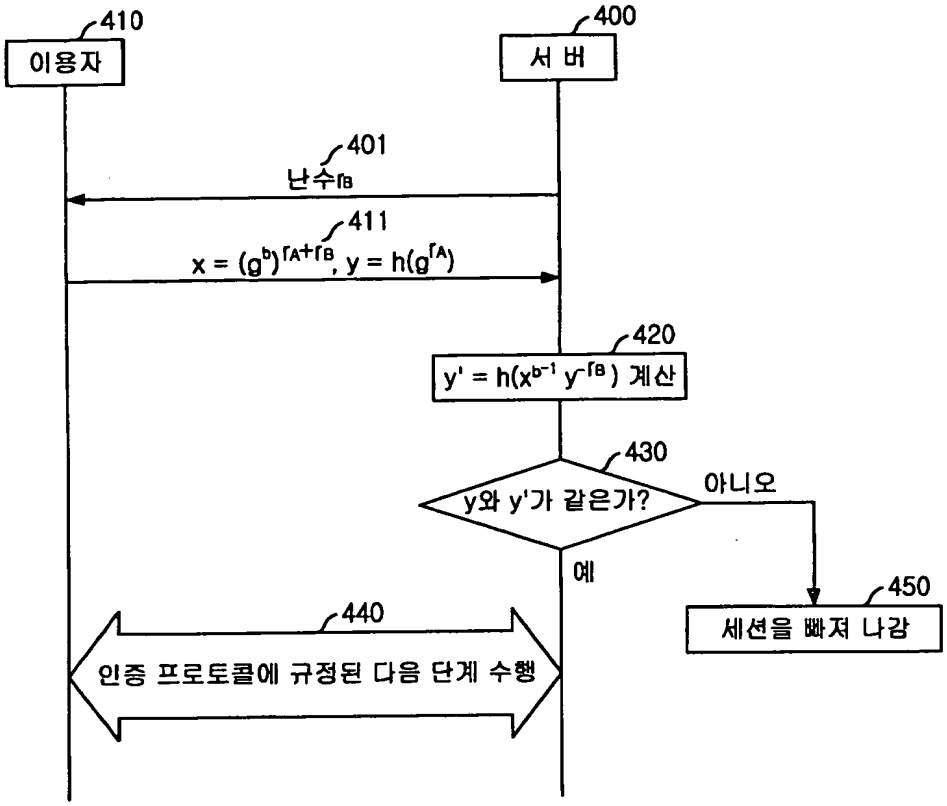
【도 2】


200
201
마스터키 (K_{master})
202
난수r_B 의 인덱스(index_r_B)
해쉬함수
(H)
203
난수r_B

【도 3】


320
이용자
310
서 버
321
서비스 요구
330
$r_B = H(K_{master}, index_r_B)$계산
331
r_B, $index\_r_B$
340
·임의의 난수 r_A 선택
·암호문 $\{r_A, r_B\}_{KB}$ 생성
350
$index\_r_B$ 값 증가
341
$index\_r_B$, 암호문 $\{r_A, r_B\}_{KB}$
360
$r_B = H(K_{master}, index\_r_B)$
계산 또는 검색 테이블에서
검색
370
r_B의 해독된
값과 r_B의 계산된 값이
서로 같은가?
아니오
예
380
인증 프로토콜의 다음 단계
수행
390
세션을 빠져 나감

【도 4】


410
이용자
400
서 버
401
난수r_B
411
$x = (g^b)^{r_A+r_B}$, $y = h(g^{r_A})$
420
$y' = h(x^{b-1} y^{-r_B})$ 계산
430
y와 y'가 같은가?
아니오
예
450
세션을 빠져 나감
440
인증 프로토콜에 규정된 다음 단계 수행